Response to Reviewer #1

We are glad that the reviewer finds our work interesting and recommended it for publication. We thank the reviewer for the insightful comments that have helped us improve the manuscript. We address the reviewer's comments in order below, as numbered by the reviewer.

1. Change the title of the paper so that it mentions "distance vector" and "interception" or "eavesdropping". Otherwise, this paper will never be found nor cited.

We agree and have changed the title to "Interception in Distance-Vector Routing Networks".

2. Deeply revise the abstract and the introduction, focusing on distance vector protocols and their security issues and citing the appropriate literature in this domain rather than BGP scenarios.

We have endeavored to revise the abstract and the introduction thoroughly, and have better located our work in the literature. In particular, we motivate our study by referring to the broad literature of routing security issues, emphasize on the connection to distance-vector routing protocols, and discuss the scope of our work and its contribution to the community.

3. Avoid "black holes" for all paths that can be chosen by non-colluding agents. This could imply also assuming some rule to break the ties (for example, RIP routers stick with the first shortest announcement they receive).

We thank the reviewer for identifying this confusing point in the paper. In our model the honest agents break ties by uniform random choice on a per-message basis (in our edits we made this much clearer in section 3). The reviewer expressed a preference for a model in which ties are broken in an arbitrary worst-case fashion. However, it is the random tie-break assumption that allows for the elegant mathematical analysis in the paper. Also, our intention is that honest agents in our model are as naïvely helpful as possible. It would be very interesting to see if our results extend to arbitrary worst-case tie-breaks or first-come-first-serve tie-breaks made by the honest agents. It is certainly plausible, however it would require more extensive analysis of the policy of the colluding agents during the synchronization protocol. Instead we can also consider different definitions of admissible strategies to avoid "black holes" for all paths chosen by honest agents. For example, we may call a strategy admissible if the length of a typical corresponding path under the strategy does not drastically differ from the length of a typical corresponding path under the honest strategy. We are exploring these directions, and certainly hope our work will inspire studies in similar directions. A related discussion is added in the last section of the paper.

4. Possibly include results on non-uniform agents sketched above (provided they are correct).

This is a great point. However, we decide not to include it in the revision for the following reason. As currently stated in the paper, the proof that deals with the reduction from the non-uniform model to the uniform model proves that the non-uniform model (in either adjacent or non-adjacent cases) reduces to the uniform model with adjacent colluding nodes. However, the non-adjacent non-uniform case does *not* reduce to the non-adjacent uniform case. It is true that, as the reviewer points out, an admissible strategy for the uniform model in Figure 5 right (when the center node is honest) is also admissible for the corresponding non-uniform model, but the strategy is not necessarily optimal for both models. Generally we do not have a "bijection" between the non-adjacent non-uniform case and the non-adjacent uniform case, in contrast to the reduction from the non-uniform model to adjacent uniform model where in some sense we do have a bijection.

MINOR COMMENTS:

- *Page 4, line 53: itself -> themselves*
- *Page 5, formula (3.1): the case when rho is equal to one can be omitted (j announces 0 to i at time t=0 and i announces 1 to its neighbors at time t=1).*
- *Page 5, line 38: "Observe that..." in this phrase both y and t are used as destinations.*
- *Page 7, caption of Fig. 3: "rho" -> "ρ"*
- *Page 12, line 13: "For a set X and an integer j" -> "For a set of integers X and an integer j"*

Above suggestions are implemented in the revision.

- *Page 9, lines 14-17: "Although nonuniform lies might appear at first glance to provide a substantial increase in power ..." this phrase is not comprehensible. Reducing the problem of finding the optimal strategy for an instance G in the nonuniform model to the analogous problem in the uniform model for an instance G' does not imply that uniform and nonuniform strategies have the same power.*

We mean "equally powerful" in the sense of a computational reduction. That is, an algorithm that "solves" the uniform case in full generality will also solve the non-uniform case in full generality. In this sense the two problems are equally difficult, since each is a special case of the other. We have updated the prose to clarify this.